UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/884,636	06/19/2001	David Otto Lewis	ROC920000168US1	2654

7590 06/03/2005

James R. Nock
IBM Corporation, Dept.917
3605 Highway 52 North
Rochester, MN 55901-7829

EXAMINER	
GURSHMAN, GRIGORY	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/884,636	LEWIS ET AL.	
	Examiner	Art Unit	
	Grigory Gurshman	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *10-55 and 97-127* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-55 and 97-127* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/19/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

Applicant in the response filed 5/11/2005 has provisionally elected Group II – claims 10-55 and 97-127.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 10-16, 18-26, 28-35, 44-49, 51-55, 97-115, 117-126 are rejected under 35 U.S.C. 102(b) as being anticipated by Fischer (U.S. Patent No. 4.868.877).

3. Referring to the instant claims, Fischer discloses a public key signature cryptosystem with enhanced digital signature certification (see abstract and Fig. 2). Fischer teaches the system for certifying digital signatures such that requirement for further joint certifying signatures is made apparent to any receiver of a digital message. The requirement for joint signatures is especially useful in transactions where money is to be transferred or authorized to be released. To accomplish this end, the certificate of the present invention is constructed to reflect (in addition to the public key and the name of the certifiee and other fields) the number of joint signatures required and an indication as to the identity of qualifying joint signers. Thus, an explicit list of each of the other public key holders that are required to sign jointly may be included in the certificate. In

this fashion, the recipient is informed that any material which is signed by the authority of the sender's certificate, must also be signed by a number of other specified signators. The recipient is therefore able to verify other joint and counter signatures by simply comparing the public keys present in each signature in the certificate. The present invention also includes other ways of indicating co-signature requirements such as by indicating other certificates. Such indications of other public key holders may be explicit (with a list as described here), or implicitly, by specifying some other attribute or affiliation. This attribute or affiliation may also be indicated in each co-signer certificate (see column 4, lines 40-65 and Fig. 3).

4. Referring to the independent claims 10, 20, 44, 51, 97, 106, 117, the limitation "descriptor data associated with the tangible object" is met by signature packet 42 in Fig. 3. The limitation "... the descriptor data including an identity public key ~~fro~~ for transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning the tangible object, and a digital signature" is met by object 20, and blocks 22, 24, 26, 28 and 40 in Fig. 3. The limitation verifying that the digital signature matches the identity public key and the attribute data" is met by process depicted in Fig. 3. The limitation "performing a first data transformation according to the first public/private key encryption algorithm using the identity public key" is met by hashing of data in block 32 (Fig. 3). The limitation " ...perform a second data transformation according to the first public/private key encryption algorithm using the identity private key" is met by decryption with the private key performed in the block 84 (see Fig. 4). The limitation "comparing the source test data with the resultant test

data" is met by block 56, comparing the data from blocks 50 and 54 in Fig. 3. The limitation "using the attribute data" is inherently met by Fischer, because he teaches that the comment (26 in Fig. 3) is included as a part of the descriptor data associated with the tangible object (20).

5. Referring to the independent claims 44, 97 and 106, the limitations "programmable processor; a memory for storing instructions ...; a digital protection system interface coupled to the processor " is met by Fig. 1.

6. Referring to claims 11, 21, 30, 47, 48, 113, 118, the limitation "decrypting the digital signature according to the second public/private key encryption algorithm using a signature public key" is met by decryption performed in block 84 using public key 90 (see Fig. 4). The limitation "comparing the decrypted digital signature to the data derived from the identity public key and the attribute data..." is met by Fig. 3 (block 56).

7. Referring to claims 12, 22, 104, 119, Fischer teaches that algorithm comprises a hash function 34 (Fig.3).

8. Referring to claim 14, 15, 24, 25, 38, 39, 54, 114, 115, Fischer teaches the data transformation processes being encryption and decryption.

9. Referring to claims 100-102, 112 and 126, it is well known in the art to use identification data derived from biometric characteristics such as retina scan, iris scan, voice sample etc. One of ordinary skill in the art would have been motivated to us retina scan, iris scan, voice sample because they uniquely identify an individual.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 17, 27, 36, 37- 43, 50, 116, 127 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (U.S. Patent No. 4.868.877) in view of Naccache (U.S. Patent No. 5.910.989).

12. Referring to the instant claims, Fischer discloses a public key signature cryptosystem with enhanced digital signature certification (see abstract and Fig. 2). Fischer teaches the system for certifying digital signatures such that requirement for further joint certifying signatures is made apparent to any receiver of a digital message (see Fig. 3). the limitation "descriptor data associated with the tangible object" is met by signature packet 42 in Fig. 3. The limitation "... the descriptor data including an identity public key fro transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning the tangible object, and a digital signature" is met by object 20, and blocks 22, 24, 26, 28 and 40 in Fig. 3. The limitation verifying that the digital signature matches the identity public key and the attribute data" is met by process depicted in Fig. 3. The limitation "performing a first data transformation according to the first public/private key encryption algorithm using the identity public key" is met by hashing of data in block 32 (Fig. 3). The limitation " ...perform a second data transformation according to the first public/private key

encryption algorithm using the identity private key" is met by decryption with the private key performed in the block 84 (see Fig. 4). The limitation "comparing the source test data with the resultant test data" is met by block 56, comparing the data from blocks 50 and 54 in Fig. 3. The limitation "using the attribute data" is inherently met by Fischer, because he teaches that the comment (26 in Fig. 3) is included as a part of the descriptor data associated with the tangible object (20). While Fischer teaches comparing source test data with the resultant test data for verifying the digital signature, he does not explicitly teach using the random source data.

13. Referring to the instant claims Naccache discloses a method for the generation of electronic signatures (see abstract). Naccache teaches an electronic signature method, comprising the generation of a digital signature by a signer unit that computes this signature by using a random data element sent by a verifier unit, and the checking of the signature by the verifier which ascertains that a mathematical condition, bringing into action the signature sent and the random data element (see column 3, lines 29-33).

Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to modify the system for digital signature verification of Fischer by using the random source test data and comparing the random source test data with the resultant test data as taught in Naccache. One of ordinary skill in the art would have been motivated to modify the system for digital signature verification of Fischer by using the random source test data and comparing the random source test data with the resultant test data as taught in Naccache for using mathematical condition method of verification of digital signatures (see column 3, lines 32-33).

14. Referring to claim 41, Fischer teaches that algorithm comprises a hash function 34 (Fig.3).

15. Referring to claim 42, it is well known in the art to use SHA-1 and MD5 algorithms. One of ordinary skill in the art would have been motivated to use SHA-1 and MD5 algorithms for hashing the information in order to use the standard hardware.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

G.G.

GG

Grigory Gurshman
Examiner
Art Unit 2132

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100